1-1-2011

Guidelines for the digital forensic processing of smartphones

Khawla Abdulla Alghafli
Khalifa University of Science, Technology and Research (KUSTAR), United Arab Emirates

Andrew Jones
Edith Cowan University

Thomas Anthony Martin
Khalifa University of Science, Technology and Research (KUSTAR), United Arab Emirates

DOI: 10.4225/75/57b2b82a40ce7
9th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, 5th -7th December 2011

GUIDELINES FOR THE DIGITAL FORENSIC PROCESSING OF SMARTPHONES

Khawla Abdulla Alghafli[1], Andrew Jones[1, 2], Thomas Anthony Martin[1]
[1] Khalifa University of Science, Technology and Research (KUSTAR), United Arab Emirates
[2] Edith Cowan University, Perth Western Australia
khawla.alghafli@kustar.ac.ae

Abstract

Today Smartphone devices are widespread and they hold a number of types of information about the owner and their activities. As a result of the widespread adoption of these devices into every aspect of our lives they can be involved in almost any crime. The aim of digital forensics of Smartphone devices is to recover the digital evidence in a forensically sound manner so that the digital evidence can be presented and accepted in court. The digital forensic process consists of four phases which are preservation, acquisition, examination/analysis and finally presentation. In this paper we look at various types of crime and their associated digital evidence. The digital forensics process of the Smartphone devices is discussed and, this paper also contains recommended guidelines and procedures for how to perform the phases of the digital forensics process on Smartphone devices. Finally, a description of some challenges that may be faced in this field is given.

Keywords

Digital forensics, Digital evidence, Preservation, Acquisition.

INTRODUCTION

Smartphone devices have seen a remarkable growth in popularity and are now involved in most aspects of our daily life. They now hold variety types of information about the activities of the owner. Examples of this information are media files, chat logs, browsing history and call history. In many cases, criminals have moved to take advantage of these devices. The usage of Smartphone devices in criminal activities is on the increase. Famous examples of these crimes are the Mumbai terrorist attack 2008 and the riots in London 2011. As a result, forensics researchers are working on finding acceptable methods to recover potential digital evidence about user activities from these devices.

The digital forensics of the Smartphone devices is a growing field due to the rapid development in Smartphone device technologies. The purpose of digital forensics research is to find accepted methods to recover the digital evidence in a forensically sound manner so that the recovered digital evidence can be presented and accepted in the court. The digital forensic field is usually called computer forensics and the definition is the following:

"Computer forensic is the collection, preservation, analysis, and presentation of computer-related evidence" (Vacca, 2010).

Today, Smartphone devices are similar in functionality to computers, but there are some differences between the digital forensics of computer devices and that of Smartphone devices. These differences are illustrated in Table 1.

Table 1. A Comparison of Computer and Smartphone Forensics

Aspect	**Computer Forensics**	**Smartphone Forensics**
Source of evidence	- Hard disk. - RAM. - External memory cards.	- Internal memory. - SIM. - External memory cards.
Can remove the internal storage media	Yes the hard disk can be removed easily.	No.

Operating system	Limited number of operating systems.	Wide range of operating systems.
Can bypass the authentication password	Yes.	Cannot bypass the authentication password during logical acquisition.
Power and data cables	Standard power and data cables.	Wide range of power and data cables.
File system	Standard file system such as FAT.	Wide range of file system.

From Table 1, it's clear that the digital forensics of the Smartphone devices is more complex than the digital forensics of computers.

POTENTIAL DIGITAL EVIDENCE IN THE SMARTPHONE DEVICES

Digital evidence is defined as "Any data that can establish that a crime has been committed or provide a link between a crime and its victim or a crime and its perpetrator" (Casey, 2004). Another definition is "any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi" (Casey, 2004).

The following are types of potential digital evidence that may be found in the Smartphone devices:

- Call history

The call history provides an insight to the call activity of the owner before the acquisition of the Smartphone device. The investigator can see in-coming, out-going and missed calls including their time and durations. This can help the forensics investigator to draw indirect conclusion about the suspected activities.

- Contact list

The contact list not only provides contact names and their numbers either home, mobile and work but also many other types of information such as contact title, company, address and emails. Also, some Smartphone devices store a picture of the contact in the contact list. The information that is stored in the contact list provides the investigator with the social and work relations of the owner of the Smartphone device. Beside this, many people store different types of account information and their passwords in the contact list. For example, email accounts or bank account pin codes.

- Text messages/ Emails

Contrary to the call history and contact list which provide indirect information, text messages and emails give explicit information that can be used as evidence in the court. This is because they contain the exact text intended to or sent by the owner of the Smartphone device.

- Media (pictures, videos, audio)

Media files such as pictures and videos can be used as potential digital evidence in the court. Many Smartphone devices such as iPhones embed the GPS co-ordinates of the location into the metadata called Exchangeable File Format (Exif) of the resulting image file (Valli & Hannay, 2010). Not only are the GPS co-ordinates stored but also valuable information for the investigator such as the date and the time of capturing. This provides the investigator with more insight of the activities of the owner of the Smartphone.

- Browsing history/internet search

The browsing history and internet searches in the Smartphone device give the investigator a picture of the internet activities of the owner. The investigator will discover the types of web sites that the owner has visited. Also, some Smartphone devices give the owner the ability to save their favorite web sites.

- Chat logs

There are several chat applications that can be installed in the Smartphone device such as Windows Live Messenger, Google Talk and BlackBerry Messenger. Users of these applications usually choose to save the chat logs. The chat logs can be used as digital evidence in the court as to what the owner said.

- Social network accounts

Most Social networks are available on Smartphones, including the most famous of all, Facebook. In this type of account the investigator can find pictures and notes that were published by the owner. Also, they can discover the owner's friends and the groups that they belong to.

- Calendar\ notes

The calendar gives a picture of the previous, current and future planned activities of the owner of the Smartphone. The calendar can be used to associate the owner of the Smartphone to specific locations and times in order to look for possible witnesses. The owner of the Smartphone may also have saved notes that have valuable information that can be presented as evidence in the court.

- Connections (mobile network, Wi-Fi, Bluetooth)

These will give the investigator an overview of the networking activities that were performed by the owner's Smartphone device. The mobile network will give a picture of which country or region the owner has roamed in. Wi-Fi will give a picture of which Local Area Network (LAN) the Smartphone connected to. Bluetooth will give the forensic investigator information about the nicknames of the devices that were connected with owners Smartphone using Bluetooth connection.

- Maps (locations, directions help, favourites)

This will provide the investigator with a geographical view of the owner's movements which can be used as potential evidence in court.

- Software (Document processing software, VoIP software, etc.)

Document processing software such as Word To Go and Sheet To Go can be used to create or edit documents that may be useable as potential digital evidence. VoIP applications such as Skype give the owner of the Smartphone the ability to communicate with many people using the IP protocol without leaving a record in the call history on the device. The suspect may use this software in communication with a criminal or a victim. For example in child abuse cases, the criminal may communicate with the child using VoIP software. The investigator has to check these applications on the suspects Smartphone device. The checks should include finding the suspects account and the associated contact list.

The forensic investigator's aim is to find evidence of the crime. There are many types of crime that may be found in computing environments. In (Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders, 2009), the document details several crimes and the associated types of digital evidence. Table 2 illustrates several examples of digital crimes and their associated potential evidence.

Table 2. Crimes in the computing environment

Name of Crime	Description	Potential computer evidence
Child abuse	The wrong treatment and usage of the children that may affect their development and their psychology.	-Internet history logs. -Chat logs. -Internet searches. -Images. -Movies files. -calendars/notes.
Murder	Killing someone intentionally.	-calendars/notes. -Internet history logs. -Address books. -Images. -Financial/asset records. -Medical records. -Reproductions of signature.

Harassment	Behavior that leads to bothering or disturbing someone.	-calendars/notes. -Internet history logs. -Address books. -Images. -Financial/asset records. -Internet searches about victims.
Identity theft	Types of crimes that aim to steal personal information such as credit card numbers and bank account numbers.	-Credit card information. -Electronic money transfer. -Financial records. -Online banking software. -Reproductions of signature. -Forged document.
Counterfeiting	Illegal actions that aim to produce imitations that look like an original .	-Credit card information -Financial records. -Reproductions of signature.
Narcotics	Types of illegal drugs that stop some of the brain functionality and relieve pain.	-Credit card information -Electronic money transfers. -Financial records. -Fictitious identification. -Photographs of drugs and accomplices. -Unfilled prescriptions.
Terrorism	Dangerous actions against civilians in order to achieve political, organization goals.	-Credit card information -Electronic money transfers. -Financial records. -Fictitious identification. -VOIP software.

DIGITAL FORENSICS PROCESS OF SMARTPHONE DEVICES

The digital forensic process consists of four phases as shown in Figure 1.

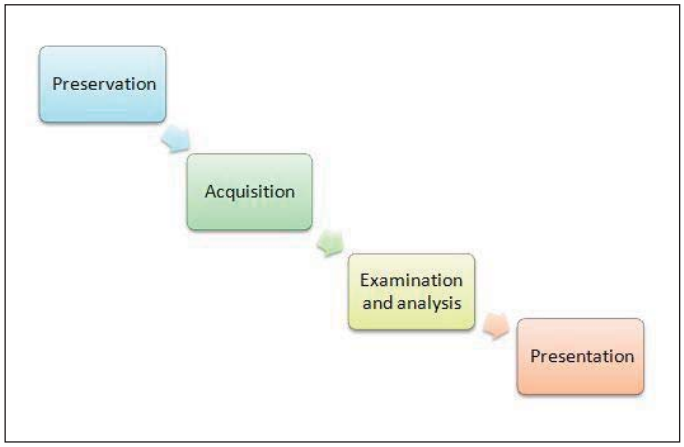

Figure 1. Digital Forensics process

In this section we discuss some guidelines to be followed in the phases of the digital forensics process of Smartphone devices.

Preservation

In the evidence preservation phase, the forensics investigator must preserve the Smartphone device in its original state. This means that no data should be changed on the device after preserving the scene. Figure 2 shows a work flow to be followed in this phase.

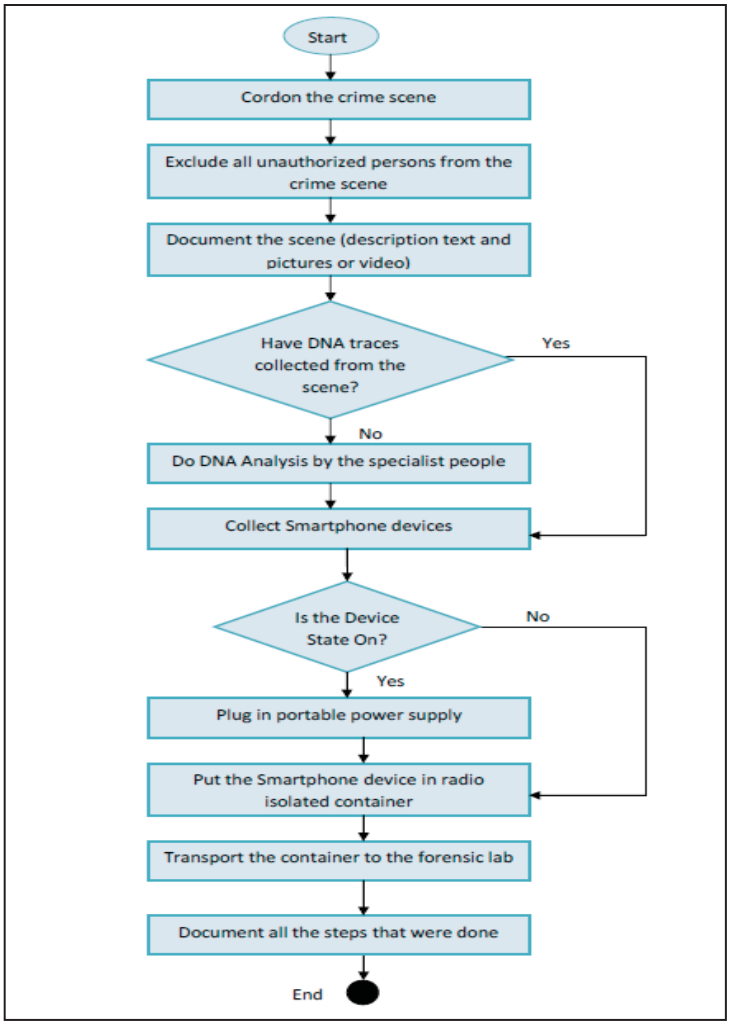

Figure 2: Work flow in the preservation phase

It is important to preserve the source of the digital evidence in its original state. Any failure to preserve the evidence in its original state at this stage will result in a failure in all of the following stages of the digital forensics process.

If the state of the device is ON the investigator should plug in a portable power supply. Consequently, it will be kept on its original state and no loss of data will occurs if the device runs out of battery. The device has to be packaged in a radio frequency isolated container (Faraday container). This is because the suspect may make the of any signal to modify or delete the evidence on the device. Also, any incoming calls may result in the overwriting of evidence. The investigator should also document all the steps that were undertaken at this stage.

Acquisition

This stage of the process starts when the device is received at the forensic lab after proper preservation, packing and transportation. Figure 3 shows a work flow to be followed in this phase.

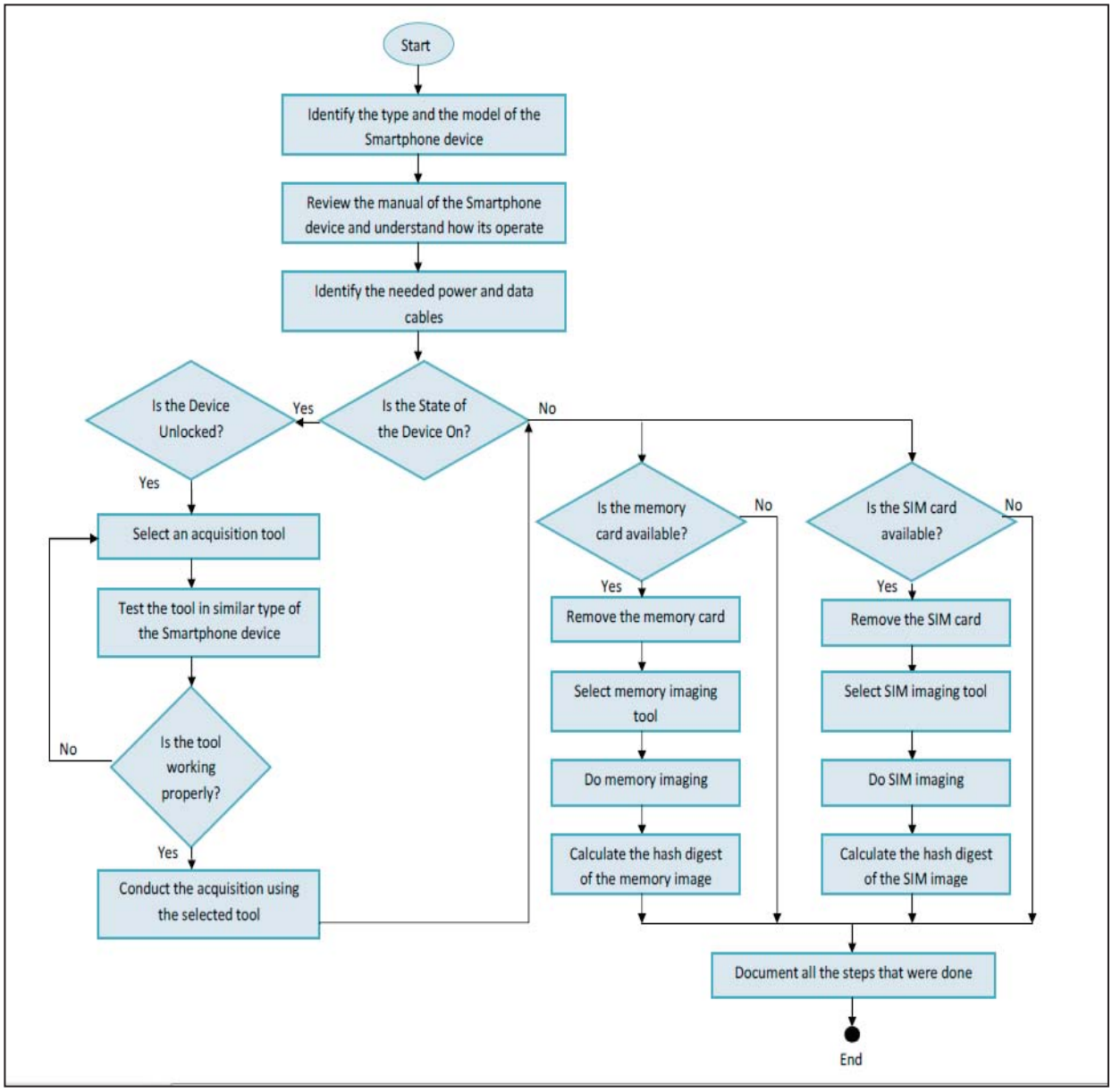

Figure 3: Work flow in the preservation phase

One of the first tasks to be undertaken in this stage is to identify the type and the model of the device. Once this has been done, the forensics examiner will be able to choose the right acquisition tool for the device. This is not easy due variety of models of Smartphone devices in market. Also there are a wide range of cloned devices that look like the original, but operate in a different manner.

The examiner should review the device's manual, understand how the device operates and what the appropriate power/data cables are for use with the device.

Once an image has been created, the integrity of the image must be checked. The most common method used is to check the integrity of a file by using a hash function. The hash function will produce a hash digest of acquired data. If any changes are made to the acquired data, the hash digest will change. Consequently, proving that no changes have taken a place since the evidence was collected is easy by using hash functions.

Furthermore, all of the steps that were undertaken must be documented.

Examination and Analysis

In this phase the forensic investigator should decide which tools they will use to support the forensic examination and analysis. For analyzing Smartphone devices, the forensic analyst can use a range of tools such as Oxygen Phone manager, Paraben Cell Seizure, Susteen Secure View or XRY (Phone manager II, 2011) (Device Seizure v4.1, 2011) (What is XRY?, 2011) these tools work with some Smartphone devices in a proper manner and others not. Thus, the forensics examiner should choose the correct tool for each type of Smartphone devices. The most important thing to be clear on that as the storage media size is increasing, the forensic process will become slower. That is because there is an increasing volume of data to be examined. According to M. G. Solomon et al. "There is no easy answer to the question "where do I look for evidence?" as with any investigation, not all evidence is clear and easily available" (Solomon, Barrett, & Broom, 2005). The answer of where to look is dependent on the type of the crime. For instance, if the crime is child abuse the investigator would focus their search on chat log files, email files and picture files. These files will, potentially, provide the investigator with a great view of system activity.

Presentation

The fourth phase in the forensic process is that of presenting the evidence. It occurs after the results have been found in the examination and analysis phase. Thus, the presentation of evidence phase shows the results that are found in the analysis phase. The duty of the forensic investigator in this phase is to prove to the audiences one or more facts using the evidence that they have obtained. They should produce a well organized report of their findings. Also, in the presentation they should explain the computer evidence in a way that can be understood by audiences that may have poor background of computer technology. The forensics examiner should also know as much as possible of the background of his audience before preparing the presentation (Solomon, Barrett, & Broom, 2005). Different types of audience have different type of expectations. For example, the expectations of managers in a company are differ from the expectations of a jury in the court. By knowing the audience, the investigator can prepare a more convincing presentation.

THE CHALLENGES OF THE DIGITAL FORENSICS OF THE SMARTPHONE DEVICES

The analysis of Smartphone devices is a rapidly growing field in digital forensics. In (Zareen & Baig, 2010) (Raghav & Saxena, 2009), several challenges are mentioned and also difficulties that are faced in this field. Some of them are:

- There is a rapid change in the technology of Smartphone devices. Today, there are a huge number of Smartphone models on the market. This has led to increasing problems in developing and maintaining a scientifically sound method for the capturing of data from these devices.
- There are a large number of different operating systems for Smartphone devices. Some of these are open source and others are not. For example, the Android is an open source operating system and Blackberry OS is a closed source operating system. How closed source operating systems work is obviously less well understood. Thus, the forensic investigator will not have a clear idea of how these operating systems are storing, modifying and retrieving data. Therefore, there is a need to perform an operational analysis of each operating system of Smartphone devices in order to understand where the data is stored and how it can be retrieved.
- The forensics investigator has to be aware that there are many tools and techniques that may be remotely used by the suspect or criminal to modify or destroy data that is held by the Smartphone. To avoid this problem, the forensic investigator has to keep the Smartphone in a signal isolated box while it is moved from the scene to the forensic lab.
- Signals to and from the Smartphone need to be blocked at the time of seizure to prevent any possible modification of the data in the device. The challenge here is that the battery life of the Smartphone is limited and placing the device in isolation will result in the battery being drained. This is because once the Smartphone is isolated, it starts searching for a mobile network. The solution to this situation is that the forensic investigator should have a portable power supply for the various models of the Smartphone. Before isolating the Smartphone, the investigator should attach the portable power supply.

- There are a wide range of data and power cables that are used by Smartphone. This can cause logistical problems and also causes confusion to a forensic investigator over which type of cables to use. To meet this challenge, a database of each Smartphone model and its appropriate cables can be created. This will simplify the process of finding the appropriate cables for each model and keep the device in its original state. However, the problem that will arise is that the forensic investigator has to carry with him a bag that contain all possible portable power supply cables before going to the crime scene.
- There is a need for a forensics tools for the acquisition of data in the case of physically damaged Smartphone devices. Most of the current tools work only with undamaged Smartphones.
- Most Smartphones have an authentication code to prevent unauthorized access. This can cause delays in accessing the Smartphone data. Also, if the number of tries to enter right code is exceeded, the Smartphone may wipe itself. To address this challenge, there is a need to develop methods that bypass the authentication code on each of the Smartphone models.
- Most of the current Smartphone forensics tools provide for the logical analysis of data. This type of analysis does not retrieve deleted files. There is a need for the development of forensic tools for each type of Smartphone device that can perform a physical analysis which can retrieve deleted data.

CONCLUSION

The fast development in Smartphone device technology is making the digital forensic of these devices a very complicated task. Also, this development leads to increasing problems in developing and maintaining a scientifically sound method for the capturing of data from these devices. We have provided guidelines to be followed in the digital forensics process, but this field has many challenges that need to be addressed. Also, there is a need to develop standard procedures to be followed by the forensic investigator and examiner in order to preserve evidence's integrity and recover it correctly, so that it can then be accepted in court.

REFERENCES

(2004). In E. Casey, *Digital Evidence and Computer crime* (pp. 12-13). Academic press.

Device Seizure v4.1. (2011). Retrieved from Paraben Corporatio: http://paraben-forensics.com/device-seizure.html

(2009). *Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders.* The National Institute of Justice.

Phone manager II. (2011). Retrieved from Oxygen Software: http://www.oxygensoftware.com/

Raghav, S., & Saxena, A. K. (2009). Mobile Forensics: Guidelines and Challenges in Data Preservation and Acquisition. *IEEE student Conference on Research and Development (SCOReD 2009)*, (pp. 5-8). Malaysia.

Solomon, M. G., Barrett, D., & Broom, N. (2005). In *Computer Forensics, jump start* (pp. 73-155). SYBEX.

(2010). In J. R. Vacca, *Computer Forensic, computer crime scene investigation* (pp. 3-31). Charles River Media.

Valli, C., & Hannay, P. (2010). Geotagging Where Cyberspace Comes to Your Place. *Security and Management 2010*, (pp. 627-632).

What is XRY? (2011). Retrieved from Micro Systemation: http://www.msab.com/xry/what-is-xry

Zareen, A., & Baig, S. (2010). Mobile Phone Forensics Challenges, Analysis and Tools Classification. Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE.2010), (pp. 47 – 55)